CHAPTER: 700

Operational Security

DEPARTMENT ORDER:

706 – Emergency Preparedness, Response, and Incident Command System (ICS)

OFFICE OF PRIMARY RESPONSIBILITY:

DD

Effective Date:

August 20, 2018

Amendment:

N/A

Supersedes:

DO 706 (9/1/96)

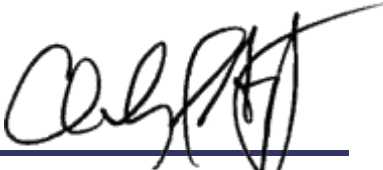**Scheduled Review Date:**

July 1, 2019

ACCESS

☐ **Contains Restricted Section(s)**

Arizona Department of Corrections

Department Order Manual

Charles L. Ryan, Director

TABLE OF CONTENTS

PURPOSE

The Department of Corrections utilizes the Incident Command System (ICS) to prepare for, prevent, respond to, recover from, and mitigate incidents and emergencies. Developed in accordance with the Federal Emergency Management Administration (FEMA), the Department's ICS provides guidelines for addressing incidents, ranging from small-scale local incidents to coordinated responses involving multiple jurisdictions. This Department Order establishes:

- The Department's ICS framework.

- Responsibility for emergency response plan development and compliance.

- Training and exercise requirements.

APPLICABILITY

This Department Order applies to:

- All Department staff and contract employees.

- All Department facilities, administrative offices, and field operations.

- Any other individuals present at the time of an incident or exercise, including but not limited to volunteers, visitors, and vendors.

This Department Order applies to Private Prisons.

RESPONSIBILITY

Only the Director has the authority to approve any instance in which an outside agency may have direct contact with an inmate outside the secure perimeter of an institution.

The Deputy Director shall have overall responsibility for the Department's Emergency Planning and Response Program, including the use of ICS.

The Division Director for Prison Operations shall ensure that all Wardens:

- Develop and maintain an Emergency Operations and Response Plan for their institution and establish the necessary collaborative relationships with local resource partners and community stakeholders to facilitate planning, response, and training opportunities.

- Collaborate with the Division Director for Inmate Programs and Reentry to ensure that on and off-site Arizona Correctional Industries (ACI) operations are appropriately addressed in prison Emergency Operations and Response Plans.

- Collaborate with the Assistant Director for Health Services Contract Monitoring Bureau to ensure that all Health units and Inpatient Care units are appropriately addressed in the prison Emergency Response Plans.

The Division Director for Inmate Programs and Reentry shall ensure that Administrators collaborate with the Emergency Preparedness Administrator to develop and maintain an Emergency Response and Operations Plan for Reentry Centers, Community Corrections Offices, and the Arizona Correctional Industries administrative offices.

The Division Director for Administrative Services shall ensure that the Chief Information Officer (CIO) develops and maintains an Information Technology (IT) Continuity Plan.

The Contract Beds Operations Director shall ensure that Wardens of Private Prisons develop and maintain an Emergency Operations and Response Plan for their prison and establish the necessary collaborative relationships with local resource partners and community stakeholders to facilitate planning, response, and training opportunities in accordance with Department Order #106, Contract Beds.

The Emergency Preparedness Administrator shall:

- Manage the Department's Emergency Preparedness and Incident Response Program.

- Assist in the coordination of ICS-oriented training and exercises.

- Collaborate in the development and maintenance of the Emergency Action Plan and Procedures for all Central Office locations, Community Corrections and regional community corrections offices, the Correctional Officer Training Academy (COTA), and Arizona Correctional Industries (ACI) administrative offices.

- Facilitate the development and maintenance of the Central Office Continuity of Operations Plan (COOP).

The Deputy Director, Division Directors, Assistant Director, Regional Operations Directors, Wardens, and Bureau Administrators shall ensure that employees complete the mandatory ICS training as outlined in the Department's Annual Training Plan.

All staff shall be familiar with the Emergency Operations and Response Plan or the Emergency Action Plan and Procedures relevant to their work areas and assignment.

PROCEDURES

1.0   **INCIDENT COMMAND SYSTEM FRAMEWORK** – The incident command framework consists of the following elements:

    1.1   The Incident Commander:

        1.1.1   The first staff member on scene, who initiates the Incident Command System until command is transferred to a higher authority, on scene if needed, based on the incident type.

        1.1.2   Responsible for the overall management of the incident.

    1.2   Command Staff – Depending on the type of incident, the Incident Commander may activate one or more of the following command staff positions. Refer to Attachment A for additional information.

1.2.1   Safety Officer – Identifies and assesses hazardous situations; prepares safety plans and ensures messages are communicated.

1.2.2   Liaison Officer – Serves as the point-of-contact with outside agencies; monitors all operations to identify potential problems as different organizations are brought together.

1.2.3   Public Information Officer – Organizes information for news releases and conducts media briefings.

1.3   General Staff – Depending on the type of incident, the Incident Commander may activate one or more of the following general staff.

1.3.1   Operations Section Chief – Responsible for all tactical operations and implementation of the oral or written plan containing the overall strategy for managing the incident.

1.3.2   Planning Section Chief – Responsible for collection, evaluation and circulation of operational information related to the incident.

1.3.3   Logistics Section Chief – Provides resources to stabilize the incident and support personnel, systems and equipment (e.g., workspace, media briefing center, transportation, communications equipment, food, water and medical care).

1.3.4   Finance/Administration Chief – Manages all financial aspects of the incident and provides financial and cost analysis information; records personnel time; maintains vendor contracts, compensation, and claims.

2.0   WEB-BASED EMERGENCY OPERATIONS CENTER

2.1   The Department utilizes WebEOC, an internet-based crisis information management system, for incidents or pre-planned events. The system provides real-time access to critical information that can be shared during the planning, response, and recovery phases of an event.

2.1.1   ADC WebEOC incidents may be used for internal events.

2.1.2   The Director may approve access to an ADC WebEOC incident with external partners such as local, county, tribal or State Governments as appropriate.

2.1.3   The Emergency Preparedness Administrator shall be the ADC WebEOC Administrator.

2.2   The Incident Commander may activate the WebEOC for rapidly escalating events that may require additional resources or may continue across several (multi-operational) shifts.

3.0   INCIDENT MANAGEMENT AND ICS ACTIVATION

3.1   Discovering an Incident – Any individual who discovers an incident shall immediately assess the situation as follows:

3.1.1   Observe – What is happening? What is the situation?

3.1.2   Orient – What are the possible courses of action?

3.1.3   Decision – Decide which course of action to take.

3.1.4   Action – Follow through on the decision.

3.2   Incidents

3.2.1   Institutions – Staff shall follow their institution's Emergency Operations and Response Plan.

3.2.2   Central Office locations including COTA, ACI Administrative Offices, and Community Corrections - Staff shall follow the Emergency Action Plan and Procedures relevant to their work areas and assignment.

3.3   The Director shall be notified of significant incidents in accordance with Department Order #105, Information Reporting.

4.0   **CENTRAL OFFICE EVACUATIONS** – If an incident at Central Office requires an evacuation of the building, staff shall follow evacuation procedures below:

4.1   Building Coordinator shall:

4.1.1   Be responsible for planning, coordinating, preparing and leading workplace building Floor Wardens for emergencies, and implementing organized building evacuation, as needed.

4.1.2   Advise onsite First Responders regarding disabled employees, inmates, visitors and any other occupants requiring evacuation assistance and location of potentially hazardous materials.

4.2   Floor Wardens shall:

4.2.1   Be assigned to each floor and ensure the safe evacuation of all staff, inmates and any members of the public.

4.2.2   Assist occupants with safe evacuation procedures in accordance with their training and ensure disabled persons are positioned appropriately in stairwell refuge areas for First Responder rescue.

4.3   Staff supervising or responsible for inmates/work crews shall:

4.3.1   Ensure the safety and accountability of inmates by evacuating them to the designated assembly area in the building's parking lot and conducting a physical count to ensure custody and control.

4.3.2   Immediately notify the Central Office Communications Center (COCC), the COCC Supervisor, or the Emergency Preparedness Administrator, and the assigned institution for any inmate who is unaccounted for or missing.

4.4   Building Occupants shall:

4.4.1   Be familiar with the State of Arizona Emergency Response Procedures (spiral bound instructions printed on orange paper) posted throughout the buildings.

4.4.2   Know a primary and secondary evacuation route to the assigned meeting area outside the building.

4.4.3   Follow all Floor Wardens' instructions during a drill or emergency.

4.4.4   If assigned an office, exit the office, close the door, hang the orange evacuation tag on the doorknob, and exit the building.

5.0   TRAINING AND EXERCISES

5.1   All staff shall complete the required ICS training as established in Department Order #509, <u>Employee Training and Education</u> and the Annual Training Plan.

5.2   <u>Training Exercises</u> – The development of emergency exercises shall be compliant with the current Homeland Security Exercise Evaluation Program (HSEEP). Exercises shall be based upon identified threats, hazards and risks. The Emergency Preparedness Administrator shall oversee the Department's Multi-Year Training and Exercise Plan (MYTEP).

IMPLEMENTATION

The Emergency Preparedness Administrator shall provide the updated template format for the Emergency Operations and Response Plan for each institution within 30 calendar days of the effective date of this Department Order.

Wardens shall update their existing plans using the template format developed by the Emergency Preparedness Administrator within 180 calendar days of the effective date of this Department Order.

The Division Director for Prison Operations shall ensure all Emergency Operations and Response Plans are reviewed annually and updated, as necessary.

Deputy Wardens of Reentry Centers shall develop/update their existing plans using the template format developed by the Emergency Preparedness Administrator within 180 calendar days of the effective date of this Department Order.

The Division Director for Inmate Programs and Reentry shall ensure all Emergency Operations and Response Plans for Reentry Centers are reviewed annually and updated, as necessary.

Plans that are developed shall include the following annexes in Attachment C (list only).

DEFINITIONS/GLOSSARY

Refer to the Glossary of Terms

ATTACHMENTS

Attachment A – The Incident Command System
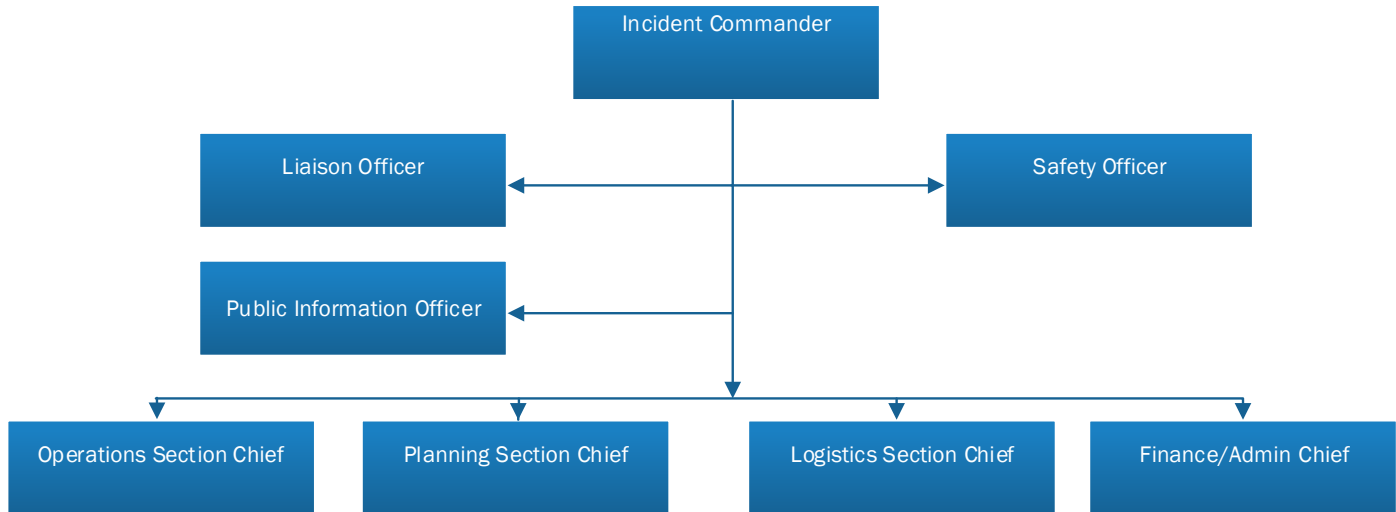Attachment B – Incident Complexity Matrix
Attachment C - Threat, Hazard, or Incident Specific Annexes

AUTHORITY

A.R.S. §41-801, Facilities Subject to Emergency Planning; Facility Emergency Response Plans

Arizona Governor's Executive Order 2013-06 Continuity of Operations and Continuity of Government Planning

National Incident Management System, Third Edition October 2017

ATTACHMENT A

THE INCIDENT COMMAND SYSTEM

```
                        ┌──────────────────────┐
                        │  Incident Commander  │
                        └──────────────────────┘
                                   │
  ┌──────────────────┐             │             ┌──────────────────┐
  │ Liaison Officer  │◄────────────┼────────────►│  Safety Officer  │
  └──────────────────┘             │             └──────────────────┘
                                   │
  ┌──────────────────────────┐     │
  │ Public Information Officer│◄────┤
  └──────────────────────────┘     │
                                   │
  ┌───────────────┬───────────────┼───────────────┬───────────────┐
  ▼               ▼               ▼               ▼
┌────────────────┐┌──────────────────┐┌─────────────────┐┌──────────────────┐
│ Operations     ││ Planning Section ││ Logistics       ││ Finance/Admin    │
│ Section Chief  ││ Chief            ││ Section Chief   ││ Chief            │
└────────────────┘└──────────────────┘└─────────────────┘└──────────────────┘
```

ATTACHMENT B

INCIDENT COMPLEXITY MATRIX

TYPE 1	• This type of incident is the most complex, requiring national resources for safe and effective management and operation. • All Command and General Staff positions are filled and management by a Type 1 Incident Management Team (IMT). • Operations personnel often exceed 500 per operational period and total personnel will usually exceed 1,000. • Branches are established for management of span of control. • A written Incident Action Plan (IAP) is required – use of WebEOC – for each operational period. A Demobilization Plan shall be developed and utilized, as well as the use of a full After Action Review/Improvement Plan. • The Director shall have briefings, and ensure the complexity analysis and delegations of authority are updated. • Use of technical specialists as resource advisors at the incident base is recommended. • There is a high impact on the local jurisdiction, requiring additional staff for office administrative and support functions.
TYPE 2	• This type of incident extends beyond the capabilities for local control and is expected to extend into multiple operational periods. It may require the response of a Type 2 IMT as well as for resources out of area, including regional and/or national resources, to effectively manage the operations, command, and general staffing, as well resources and staffing overhead. • Most or all of the Command and General Staff positions are filled. Many of the Functional Units are needed and staffed. • A written IAP is required – use of WebEOC – for each operational period. A Demobilization Plan shall be developed and utilized, as well as the use of a full After Action Review/Improvement Plan. • Operations personnel normally do not exceed 200 per operational period and total incident personnel do not exceed 500 (guidelines only). • The Director is responsible for the incident complexity analysis, department administration briefings, and the written delegations of authority.
TYPE 3	• When incident needs exceed capabilities, the appropriate ICS positions should be added to match the complexity of the incident. • Some or all of the Command and General Staff positions may be activated, as well as Division/Group Supervisor and/or Unit Leader level positions. • A Type 3 IMT or incident command organization manages initial action incidents with a significant number of resources, an extended attack incident until containment/control is achieved, or an expanding incident until transition to a Type 1 or 2 IMT. • The incident may extend into multiple operational periods. • A written IAP is required – use of WebEOC – for each operational period. A Demobilization Plan shall be developed and utilized, as well as the use of a full After Action Review/Improvement Plan.
TYPE 4	• Command and General Staff functions are activated only if needed. • Several resources are required to mitigate the incident, including a Task Force or Strike Team. Examples may include DART or TSU. • The incident is usually limited to one operational period in the control phase. • The Director may have briefings, and ensure the complexity analysis and delegation of authority is updated. • No written IAP is required but a documented Operational Briefing shall be completed for all incoming resources. No Demobilization Plan is required. Should include the use of an After Action Review form 706-2(f). • The role of the agency administrators such as the Director, Division Director, or Regional Directors may include operational plans, including objectives and priorities.
TYPE 5	• The incident can be handled with one or two single resources with up to six personnel. • Command and General Staff positions (other than the Incident Commander) are not activated. • No written Incident Action Plan (IAP) is required. No Demobilization Plan is required. May include the use of an After Action Review form 706-2(f). • The incident is contained within the first operational period and often within an hour to a few hours after resources arrive on scene.

ATTACHMENT C

THREAT, HAZARD, OR INCIDENT SPECIFIC ANNEXES

NATURAL:

Animal Related - Department Canines, Horses and Livestock
Drought
Dust Storm
Earthquake
Fissure
Flooding
Heat Wave
Hurricane
Landslide
Pandemic Outbreak
Tornado/Shear Line Winds
Tsunami
Volcanic Eruption
Wildfire
Winter Storm

TECHNOLOGICAL:

Dam/Levee Failure
Food Contamination
Hazardous Materials Spill or Release
Nuclear Substance Release
Radiological Substance Release
Utility Failure - Electrical, Natural Gas, Phone/IT Network and Water/Wastewater

HUMAN CAUSED: ADVERSARIAL OR PRISON CENTRIC:

Aircraft or Unmanned Aerial Vehicle (drone) Crash/Intrusion
Aircraft or Unmanned Aerial Vehicle as a Weapon
Armed Assault/Workplace Violence (Active Shooter)
Bomb Threat
Critical Infrastructure - Fresh Water Supply and Waste Water Treatment
Civil Unrest Outside the Institution
Death - Intentional (Homicide), Unintentional/Accidental and Natural Causes
Disturbance (Riot)
Emergency Count
Escape
Hostage
Hunger Strike
Medical Emergencies - Use of Health Services Personnel for Medical Emergencies [on Institution property], Pandemic and Closed Point of Dispensing (POD) for medical prophylaxis
Terrorism Nexus - Biological Attack, Chemical Attack, Cyber Attack Against Data, Cyber Attack Against Infrastructure, Explosives Attack, Nuclear Attack, Radiological Attack
Use of Force
Work Stoppage (Employee)